IN THE CLAIMS

1. (Currently amended) A method for monitoring abnormalities in a data stream, comprising the steps of:

receiving a plurality of objects in the data stream;

creating one or more clusters from the plurality of objects, wherein at least a portion of each of the one or more clusters comprises statistical data representative of the respective cluster, wherein the statistical data comprises a time-sensitive weight for each of the plurality of objects in each of the one or more clusters, the time-sensitive weight having a value that decreases at a specified rate such that more recently received objects are assigned a higher priority, and wherein the one or more clusters are condensed for maintenance at a high level of granularity as one or more cluster droplets;

determining from the statistical data whether each of the one or more clusters is abnormal, wherein a cluster is abnormal when no objects in the data stream are added to the cluster prior to the time-sensitive weights of the cluster decreasing to a predefined value; and

reporting at least one of the one or more clusters as an abnormal cluster of objects in the data stream;

wherein the step of creating one or more clusters further comprises:

computing one or more similarity values for a given object relating to one or more existing clusters;

determining a closest cluster for the object based on the one or more similarity values;

determining whether the similarity value for the object relating to the closest cluster is greater than a threshold;

responsive to a determination that the similarity value is greater than the threshold, adding the object to the closest cluster and updating the statistical data of the closest cluster;

responsive to a determination that the similarity value is not greater than the threshold, determining whether there is at least one cluster to which no object has been added within a given period of time;

responsive to a determination that there is no cluster to which at least no object has been added within the given period of time, adding the object to the closest cluster and updating the statistical data of the closest cluster; and

responsive to a determination that there is at least one cluster to which no object has been added within the given period of time, replacing the cluster to which no object has been added within the longest period of time with a new cluster comprising the object and generating statistical data of the new cluster.

2-4. (Canceled)

5. (Previously presented) The method of claim 1, wherein the step of determining from the statistical data whether each of the one or more clusters is abnormal comprises the steps of:

determining which clusters present at a first time were not present at a second time, wherein the second time is before the first time;

determining which of the clusters, present at the first time and not present at the second time, contain fewer than a user-defined number of objects; and

reporting clusters with fewer than the user-defined number of objects as abnormalities.

6. (Original) The method of claim 1, wherein the statistical data of each cluster is stored using an incremental updating process.

7. (Original) The method of claim 1, wherein the statistical data of each cluster comprises one or more statistical counts of each pairwise attribute.

8. (Original) The method of claim 1, wherein the statistical data of each cluster comprises one or more statistical counts of each categorical attribute.

9. (Original) The method of claim 1, wherein the statistical data of each cluster comprises a number of objects in each cluster.

10. (Original) The method of claim 1, wherein the statistical data is stored periodically at intervals chosen based on a pyramidal distribution.

11. (Original) The method of claim 1, wherein the step of creating one or more clusters further comprises the step of applying one or more weights to one or more attributes.

12. (Original) The method of claim 1, wherein abnormalities comprise intrusions in a network.

13. (Original) The method of claim 12, wherein the step of receiving a plurality of objects further comprises the step of collecting source IP (Internet Protocol) address data, destination IP address data and signature data.

14. (Original) The method of claim 12, wherein the step of creating one or more clusters further comprises the step of clustering source IP address data, destination IP address data and signature data.

15. (Previously presented) The method of claim 12, wherein the step of determining from the statistical data whether each of the one or more clusters is abnormal comprises the step of detecting one or more intrusions from statistical data of source IP address data, destination IP address data and signature data.

16. (Currently amended) Apparatus for monitoring abnormalities in a data stream, comprising:

a memory; and

at least one processor coupled to the memory and operative to: (i) receive a plurality of objects in the data stream; (ii) create one or more clusters from the plurality of objects, wherein at least a portion of each of the one or more clusters comprises statistical data representative of the respective cluster, wherein the statistical data comprises a time-sensitive weight for each of the plurality of objects in each of the one or more clusters, the time-sensitive weight having a value that decreases at a specified rate such that more recently received objects are assigned a higher priority, and wherein the one or more clusters are condensed for maintenance at a high level of granularity as one or more cluster droplets; and (iii) determine from the statistical data whether each of the one or more clusters is abnormal, wherein a cluster is abnormal when no objects in the data stream are added to the cluster prior to the time-sensitive weights of the cluster decreasing to a predefined value;

wherein the operation of creating one or more clusters further comprises:

computing one or more similarity values for a given object relating to one or more existing clusters;

determining a closest cluster for the object based on the one or more similarity values;

determining whether the similarity value for the object relating to the closest cluster is greater than a threshold;

responsive to a determination that the similarity value is greater than the threshold, adding the object to the closest cluster and updating the statistical data of the closest cluster;

responsive to a determination that the similarity value is not greater than the threshold, determining whether there is at least one cluster to which no object has been added within a given period of time;

responsive to a determination that there is no cluster to which at least no object has been added within the given period of time, adding the object to the closest cluster and updating the statistical data of the closest cluster; and

responsive to a determination that there is at least one cluster to which no object has been added within the given period of time, replacing the cluster to which no object has been added

within the longest period of time with a new cluster comprising the object and generating statistical data of the new cluster.

17-19. (Canceled)

20. (Previously presented) The apparatus of claim 17, wherein the operation of determining from the statistical data whether each of the one or more clusters is abnormal further comprises:

determining which clusters present at a first time were not present at a second time, wherein the second time is before the first time;

determining which of the clusters, present at the first time and not present at the second time, contain fewer than a user defined number of objects; and

reporting clusters with fewer than a defined number of objects as abnormalities.

21. (Original) The apparatus of claim 16, wherein the statistical data of each cluster is stored using an incremental updating process.

22. (Original) The apparatus of claim 16, wherein the statistical data of each cluster comprises one or more statistical counts of each pairwise attribute.

23. (Original) The apparatus of claim 16, wherein the statistical data of each cluster comprises one or more statistical counts of each categorical attribute.

24. (Original) The apparatus of claim 16, wherein the statistical data of each cluster comprises a number of objects in each cluster.

25. (Original) The apparatus of claim 16, wherein the statistical data is stored periodically at intervals chosen based on a pyramidal distribution.

26. (Original) The apparatus of claim 16, wherein the operation of creating one or more clusters further comprises applying one or more weights to one or more attributes.

27. (Original) The apparatus of claim 16, wherein abnormalities comprise intrusions in a network.

28. (Original) The apparatus of claim 27, wherein the operation of receiving a plurality of objects further comprises collecting source IP address data, destination IP address data and signature data.

29. (Original) The apparatus of claim 27, wherein the operation of creating one or more clusters further comprises clustering source IP address data, destination IP address data and signature data.

30. (Previously presented) The apparatus of claim 27, wherein the operation of determining from the statistical data whether each of the one or more clusters is abnormal further comprises detecting one or more intrusions from statistical data of source IP address data, destination IP address data, and signature data.

31. (Canceled).